MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2018/2019

TDF3241 – DIGITAL FORENSICS

(All Sections / Groups)

7 MARCH 2019
2.30P.M. – 4.30P.M.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 4 pages (including cover page) with 5 Questions only.

2. Attempt **ALL** questions. The distribution of the marks for each question is given. This paper carries **50 marks**.

3. Please print all your answers in the Answer Booklet provided.

Question 1 (10 Marks)

(a) You have been asked to design the content of an internal warning banner for a computer system and network. Prepare FIVE(5) examples of sentences you can include in the warning banner. [5 marks]

(b) Alfred has been asked to conduct an investigation involving email abuse. Prepare a list of FIVE (5) items he would need to obtain for an email abuse investigation. [5 marks]

Question 2 (10 Marks)

(a) You have just been appointed as a lab manager of a MyCert. Construct a list of FIVE(5) duties you have to perform to manage the computer forensics lab. [5 marks]

(b) Ezzlynn has been called to process a crime scene. Construct FIVE(5) ways or guidelines on how she should video record the computer incident or crime scene. [5 marks]

Continued ...

Question 3 (10 Marks)

(a) You have been asked to write a textbook on Windows systems. Show FIVE (5) features offered by current whole disk encryption tools. [5 marks]

(b) Why is validating evidence critical in computer forensics? [1 mark]

(c) You found an image file that you suspect is a JPEG file but it cannot be displayed with a bitmap graphics program. What can you do to recover the graphics file? [4 Marks]

Question 4 (10 Marks)

(a) You are dealing with an active network intrusion in your company. You suspect that employees are accessing network areas that are restricted and prohibited through the network. You know that live acquisitions must be used instead of the typical forensic procedure. What are the challenges you face in live acquisitions in dealing with this kind of attack? [4 Marks]

(b) You as a digital forensic investigator have determined that a crime of fraud has been committed involving e-mail in a company. What do you have to do to gather evidence for the case from e-mail? [4 Marks]

(c) When investigating an e-mail crimes, a very important step is to examine the e-mail header. What information are you looking for by examining the e-mail header? [2 Marks]

Continued ...

Question 5 (10 Marks)

(a) When a mobile device is seized, messages or calls might be received that may or may not be admissible in court. Therefore, device must be isolate from incoming signals. What are the THREE (3) options that you can use to isolate the mobile device from incoming signals? What is the drawback of using these isolating options? [4 Marks]

(b) What is the biggest challenge of mobile forensics? [2 Marks]

(c) You as a forensics examiner have been called by the court for a trial as a technical/scientific witness for a case. How should you prepare your testimony? [2 Marks]

(d) How does a deposition differ from trial testimony and what is the purpose of the deposition? [2 Marks]

END OF EXAM PAPER